



Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Almost locally free fields

Moshe Jarden

Tel Aviv University, Israel

ARTICLE INFO

Article history:

Received 5 September 2010

Available online 8 April 2011

Communicated by Aner Shalev

Keywords:

Galois group

Abhyankar's conjecture

ω -free groups

Embedding problems

ABSTRACT

Using the positive solution of the general Abhyankar's conjecture, we prove that the fundamental group $\pi_1(C)$ of the smooth connected affine curve C is "almost free". That is, for each positive integer e and for almost all $\sigma = (\sigma_1, \dots, \sigma_e) \in \pi_1(C)^e$ in the sense of the Haar measure, the closed subgroup of $\pi_1(C)$ generated by $\sigma_1, \dots, \sigma_e$ is profinite free on e generators. This implies a theorem of Harbater–Stevenson, proved by other means, that every finite embedding problem for $\pi_1(C)$ is solvable, if we restrict the problem to a suitable open subgroups.

© 2011 Elsevier Inc. All rights reserved.

Introduction

In 1953, Iwasawa characterized the free profinite group \hat{F}_ω on countably many generators as a profinite group G generated by countably many elements such that every finite embedding problem for G is solvable [Iwa53, p. 569, Thm. 5]. Following this characterization, we say that a profinite group G is ω -free if every finite embedding problem for G is solvable.

While the absolute Galois groups of most fields and even of most Hilbertian fields are not ω -free, Kuyk proves in [Kuy68, Thm. 3] that if K is a Hilbertian field and $G = \text{Gal}(K)$ is its absolute Galois group, then G satisfies the following weaker property than being ω -free:

(1) For every finite embedding problem

$$(\varphi : G \rightarrow A, \alpha : B \rightarrow A)$$

for G there exist an open subgroup H of G and an epimorphism $\gamma : H \rightarrow B$ such that $\alpha \circ \gamma = \varphi|_H$. Here A and B are finite groups and φ, α are epimorphisms.

E-mail address: jarden@post.tau.ac.il.

0021-8693/\$ – see front matter © 2011 Elsevier Inc. All rights reserved.

doi:10.1016/j.jalgebra.2011.03.021

In a recent paper, Harbater–Stevenson refer to a profinite group satisfying (1) as *almost ω -free* [HrS11, p. 1]. Thus, Kuyk's result can be reformulated by saying that if K is a Hilbertian field, then $\text{Gal}(K)$ is almost ω -free.

Kuyk's proof is generic: Without loss $A = \text{Gal}(L/K)$ for some finite Galois extension L of K . Let $(x_b)_{b \in B}$ be a set of algebraically independent elements over K . Define an action of an element $b' \in B$ on $F = L(x_b)_{b \in B}$ by $(x_b)^{b'} = x_{bb'}$ for each $b \in B$ and $l^{b'} = l^{\alpha(b')}$ if $l \in L$. This defines an action of B on F . Let E be the fixed field of B in F . Then F/E is a finite Galois extension with $B = \text{Gal}(F/E)$, $\text{res} : \text{Gal}(LE/E) \rightarrow \text{Gal}(L/K)$ is an isomorphism, and $\text{res} : \text{Gal}(F/E) \rightarrow \text{Gal}(L/K)$ coincides with α . Thus, the lifting of the original embedding problem from K to E has F as a solution field. Finally, we choose a transcendence basis $\mathbf{t} = (t_1, \dots, t_n)$ for E/K with $n = |B|$ and use the Hilbertianity of K to find a K -specialization $\mathbf{a} \in K^n$ that extends to an L -place of F such that the residue fields K', L', F' of E, EL, F , respectively, give the desired tower of fields with $\text{res} : \text{Gal}(L'/K') \rightarrow \text{Gal}(L/K)$ being an isomorphism and F' being a solution field of the lifting of the original embedding problem to K' .

Another proof of Kuyk's result can be found in [Jar74, Thm. 15.1]. That proof is based on another property that the absolute Galois group $G = \text{Gal}(K)$ of a Hilbertian field K has [Frj08, Thm. 18.5.6]:

- (2) For each positive integer e and for almost all $\sigma = (\sigma_1, \dots, \sigma_e) \in G^e$ the closed subgroup $\langle \sigma \rangle$ of G generated by $\sigma_1, \dots, \sigma_e$ is isomorphic to the free profinite group \hat{F}_e on e generators.

Here “almost all” means “all but a subset of G^e of Haar measure 0” [Frj08, Sections 18.1 and 18.2]. We call each profinite group G satisfying condition (2), *almost locally free*.

Harbater–Stevenson consider in [HrS11] an algebraically closed field of positive characteristic p and a smooth connected affine curve C . In contrast to characteristic 0, the fundamental group $\pi_1(C)$ is not free. However, they prove that $\pi_1(C)$ is almost ω -free [HrS11, Thm. 6]. Their proof uses the general Abhyankar's conjecture proved by Raynaud and Harbater (see [Hrb94]), formal patching, and manipulation of inertia groups of branch points.

The goal of this note is to show that a slight modification of the proof of [Jar74, Thm. 15.1] proves that the profinite group $\pi_1(C)$ is almost locally free and this implies that $\pi_1(C)$ is almost free, reproving the result of Harbater–Stevenson. Except of using the generalized Abhyankar's conjecture, our proof is group theoretic with a probabilistic flavor.

1. The fundamental group of a curve in positive characteristic

Given a profinite group G , we let μ_G be the unique Haar measure of G with $\mu_G(G) = 1$. Thus, μ_G is a probability measure of G . By abuse of notation we write μ_G also for μ_{G^e} for each $e \geq 1$. As usual, we say that a sequence B_1, B_2, B_3, \dots of measurable subsets of G^e is *independent*, if $\mu(\bigcap_{i \in I} B_i) = \prod_{i \in I} \mu_G(B_i)$ for each finite set I of positive integers.

Lemma 1.1. *Let G be a profinite group and S a finite group. Suppose S^m is a quotient of G for each positive integer m . Then, G has an independent sequence N_1, N_2, N_3, \dots of open normal subgroups with $G/N_i \cong S$ for each $i \geq 1$.*

Proof. Inductively assume we have constructed independent open normal subgroups N_1, \dots, N_m of G with $G/N_i \cong S$ for $i = 1, \dots, m$. We set $N = N_1 \cap \dots \cap N_m$ and let r be the number of proper subgroups of G that contain N . By assumption, G has an open normal subgroup M with $G/M \cong S^{r+1}$. Thus, G has $r+1$ open normal subgroups M_1, \dots, M_{r+1} that contain M such that $G/M_j \cong S$ and $M_j M_{j'} = G$ for all distinct $1 \leq j, j' \leq r+1$. If $M_j N < G$ for $j = 1, \dots, r+1$, then by the choice of r , there exist distinct $1 \leq j, j' \leq r+1$ with $M_j N = M_{j'} N$, so $M_j M_{j'} < G$. This contradiction implies that there exists $1 \leq j \leq r+1$ with $M_j N = G$. Setting $N_{m+1} = M_j$, we get that $(G : \bigcap_{i=1}^{m+1} N_i) = \prod_{i=1}^{m+1} (G : N_i)$. Consequently, N_1, \dots, N_m, N_{m+1} are independent [Frj08, Lemma 18.3.7]. \square

A proof of the following simple observation appears in [Hal82, Proof of Prop. 3.3]. As usual, we denote the symmetric group and the alternating group of degree n by S_n and A_n , respectively.

Lemma 1.2 (Haran–Lubotzky). *Each finite group A can be embedded in A_n for each $n \geq |A| + 2$.*

Proof. Multiplication from the right by the elements of A embeds A into S_m , where $m = |A|$ (Cayley's theorem). So, it suffices to embed S_m into A_n , for each $n \geq m + 2$. This is done by mapping each $\sigma \in S_m$ onto σ if σ is an even permutation and onto the product $\sigma(m+1 \ m+2)$ if σ is an odd permutation. \square

Lemma 1.3. *Let G be a profinite group such that A_n^m is a quotient of G for all $n \geq 5$ and $m \geq 1$. Then G is almost locally free.*

Proof. Given a positive integer e , we have to prove that $\langle \sigma \rangle \cong \hat{F}_e$ for almost all $\sigma \in G^e$.

To this end we consider a finite group A generated by e elements. We use Lemma 1.2 to embed A into A_n , where $n \geq \max(5, |A| + 2)$. Lemma 1.1 gives an independent sequence N_1, N_2, N_3, \dots of open normal subgroups of G with $G/N_i \cong A_n$ for each $i \geq 1$. For each $i \geq 1$ we choose $\bar{\sigma}_{i1}, \dots, \bar{\sigma}_{ie} \in G/N_i$ such that $\langle \bar{\sigma}_{i1}, \dots, \bar{\sigma}_{ie} \rangle \cong A$. Let $B_i = \{(\sigma_1, \dots, \sigma_e) \in G^e \mid \sigma_j N_i = \bar{\sigma}_{ij}, j = 1, \dots, e\}$. Then, $\mu_G(B_i) = (\frac{2}{n!})^e$ is positive and independent of i , so $\sum_{i=1}^{\infty} \mu_G(B_i) = \infty$. By [Frj08, Lemma 18.3.7], B_1, B_2, B_3, \dots are independent. It follows from Borel–Cantelli that $\mu_G(B(A)) = 1$, where $B(A) = \bigcup_{i=1}^{\infty} B_i$ [Frj08, Lemma 18.3.5]. Each $\sigma = (\sigma_1, \dots, \sigma_e) \in B(A)$ belongs to B_i for some $i \geq 1$. Thus, $\langle \sigma N_i \rangle = \langle \bar{\sigma}_i \rangle \cong A$, so A is a quotient of $\langle \sigma \rangle$.

Since there are only countably many isomorphism classes of finite groups, the intersection B of all the $B(A)$'s with A ranging over a set of representatives of the isomorphism classes of finite groups generated by e elements has measure 1. If $\sigma \in B$, then each finite group generated by e elements is a quotient of $\langle \sigma \rangle$. Consequently, by [Frj08, Lemma 17.7.1], $\langle \sigma \rangle \cong \hat{F}_e$. \square

Lemma 1.4. *If a profinite group G is almost locally free, then G is almost ω -free.*

Proof. Let $(\varphi : G \rightarrow A, \alpha : B \rightarrow A)$ be a finite embedding problem for G . We choose a positive integer e such that B is generated by e elements. Then A is also generated by e elements, say a_1, \dots, a_e . Since $S = \{\sigma \in G^e \mid \varphi(\sigma) = \mathbf{a}\}$ has a positive measure and G is almost locally free, there exists $\sigma \in S$ such that $\langle \sigma \rangle \cong \hat{F}_e$. In particular, $\varphi(\langle \sigma \rangle) = A$. By Gaschütz, there exists an epimorphism $\gamma_0 : \langle \sigma \rangle \rightarrow B$ such that $\alpha \circ \gamma_0 = \varphi|_{\langle \sigma \rangle}$ [Frj08, Prop. 17.7.3].

Now we choose an open normal subgroup N of G with $N \leq \text{Ker}(\varphi)$ and $N \cap \langle \sigma \rangle \leq \text{Ker}(\gamma_0)$, let $H = N \cdot \langle \sigma \rangle$, and observe that the map $\gamma : H \rightarrow B$ defined by $\gamma(v\tau) = \gamma_0(\tau)$ for all $v \in N$ and $\tau \in \langle \sigma \rangle$ is a well-defined epimorphism with $N \leq \text{Ker}(\gamma)$. Moreover, $\alpha(\gamma(v\tau)) = \alpha(\gamma_0(\tau)) = \varphi(\tau) = \varphi(v\tau)$. Thus, H is open in G and $\alpha \circ \gamma = \varphi|_H$, as desired. \square

The combination of Lemma 1.3 and Lemma 1.4 gives the following result.

Lemma 1.5. *Let G be a profinite group. Suppose A_n^m is a quotient of G for all $n \geq 5$ and $m \geq 1$. Then G is almost ω -free.*

Let p be a prime number. Recall that a finite group A is *quasi- p* if A is generated by all of its p -Sylow groups, equivalently, if A is the closed normal subgroup of itself generated by each of its p -Sylow groups.

Lemma 1.6. *Let p be a prime number. Then A_n^m is a quasi- p group for all $n \geq \max(5, p)$ and $m \geq 1$.*

Proof. Consider m isomorphic copies B_1, \dots, B_m of A_n and let $B = B_1 \times \dots \times B_m \cong A_n^m$. For each $1 \leq j \leq m$ let $B_{j,p}$ be a p -Sylow subgroup of B_j . Since $n \geq p$, $B_{j,p}$ is nontrivial and $B_p = B_{1,p} \times \dots \times B_{m,p}$ is a p -Sylow subgroup of B . Let C be the normal subgroup of B generated by B_p . Then C contains the normal subgroup of B_j generated by $B_{j,p}$. Since $n \geq 5$, B_j is a simple group, so $C \geq B_j$ for $j = 1, \dots, m$. Hence, $C = B$. It follows that B is a quasi- p group. \square

Lemma 1.5 gives the necessary tool to reprove the result of Harbater–Stevenson mentioned above.

Theorem 1.7. *Let K be an algebraically closed field of positive characteristic p . Let X be a smooth connected projective K -curve, S a nonempty set of closed points of X , and $C = X \setminus S$. Then $\pi_1(C)$ is almost ω -free.*

Proof. By the generalized Abhyankar’s conjecture [Hrb94, Thm. 6.2], each quasi- p group is a quotient of $\pi_1(C)$. Hence, by Lemma 1.6, A_n^m is a quotient of $\pi_1(C)$ for all integers $n \geq 5$ and $m \geq 1$. Hence, by Lemma 1.5, $\pi_1(C)$ is almost ω -free. \square

2. More examples

We give more examples of almost locally free profinite groups and prove preservation theorems of almost local freeness for the absolute Galois group of a Hilbertian field and for nonabelian free profinite groups.

Example 2.1. Lubotzky proved in [Lub93, Thm. 1(b)] that every free profinite group F of finite rank at least 2 is almost locally free. Hence, by Lemma 1.4, F is also almost ω -free. This is Corollary 8 of [HrS11]. Harbater–Stevenson give two proofs of the latter result. The first one depends on the structure of the fundamental groups of affine irreducible \mathbb{C} -curves, whose verification uses the Riemann existence theorem. The second proof is purely group theoretic and goes as follows: Let $(\varphi : F \rightarrow A, \alpha : B \rightarrow A)$ be a finite embedding problem for F . Choose a prime number p that does not divide the order of A and an open normal subgroup H of F such that $F/H \cong \mathbb{Z}/p\mathbb{Z}$. Then, $H \cdot \text{Ker}(\varphi) = F$, so $\varphi(H) = A$. If p is sufficiently large, then by Nielsen–Schreier, H is free of rank at least that of B [FrJ08, Prop. 17.6.2]. By Gaschütz, there exists an epimorphism $\gamma : H \rightarrow B$ such that $\alpha \circ \gamma = \varphi|_H$ [FrJ08, Prop. 17.7.3], as desired.

If F is a free profinite group of infinite rank, then every finite embedding problem for F is solvable. In particular, A_n^m is a quotient of F for all positive integers m, n . By Lemma 1.3, F is almost ω -free, reproving [HrS11, Cor. 8] in this case.

Example 2.2. We note that if a quotient G of a profinite group \hat{G} is almost locally free, then \hat{G} is also almost locally free.

Indeed, for each positive integer e , G^e has a subset S of measure 1 such that $\langle \sigma \rangle \cong \hat{F}_e$ for each $\sigma = (\sigma_1, \dots, \sigma_e) \in S$. The lifting \hat{S} of S to \hat{G}^e also has measure 1. If $\hat{\sigma} = (\hat{\sigma}_1, \dots, \hat{\sigma}_e) \in \hat{S}$ and σ is its image in S , then $\langle \sigma \rangle \cong \hat{F}_e$ and $\langle \sigma \rangle$ is a quotient of $\langle \hat{\sigma} \rangle$. By [FrJ08, Lemma 17.7.1], $\langle \hat{\sigma} \rangle \cong \hat{F}_e$.

In particular, we may take \hat{G} to be the universal Frattini cover of G . Then \hat{G} is projective. Moreover, \hat{G} is the minimal projective cover of G [FrJ08, Prop. 22.6.1]. By Lubotzky–v.d. Dries, \hat{G} is then isomorphic to the absolute Galois group of a PAC field [FrJ08, Cor. 23.1.2].

For example, we may start from the direct product $G = \prod_{n=5}^{\infty} G_n$, where G_n is the direct product of countably many isomorphic copies of A_n . By Lemma 1.3, G is almost locally free. Hence, its universal Frattini cover \hat{G} is also almost locally free. By definition, the kernel N of the map $\hat{G} \rightarrow G$ is contained in the Frattini subgroup $\Phi(\hat{G})$ of \hat{G} [FrJ08, Def. 22.5.1], and $\Phi(\hat{G})$ is pronilpotent [FrJ08, Lemma 22.1.2], hence so is N . By [FrJ08, Thm. 25.4.7], \hat{G} is not a free profinite group.

Remark 2.3. We also note that each open subgroup H of an almost locally free profinite group G is also almost locally free. Indeed, given a positive integer e , there exists a subset S of G^e with $\mu_G(S) = 1$ such that $\langle \sigma \rangle \cong \hat{F}_e$ for each $\sigma \in S$. Our observation follows now from the fact that $\mu_H(H^e \cap S) = 1$.

A Galois extension N of a Hilbertian field K is in many cases Hilbertian but not always, even if $N \neq K_s$. For example the maximal pro-2 extension $K^{(2)}$ of K is not Hilbertian, because it does not have quadratic extensions. Nevertheless, the property of $\text{Gal}(K)$ of being almost locally free is preserved under Galois extensions of K , except if they are separably closed. This consequence of Weissauer’s theorem is proved in Proposition 2.5 below:

Lemma 2.4. *Let G be a profinite group of rank \aleph_0 . Suppose each proper open subgroup of G is almost locally free. Then G is also almost locally free.*

Proof. The assumption that $\text{rank}(G) = \aleph_0$ implies that G is not finitely generated and has \aleph_0 proper open subgroups. We list them as G_1, G_2, G_3, \dots . Now we consider a positive integer e . We denote the set of all $\sigma \in G_i^e$ such that $\langle \sigma \rangle \cong \hat{F}_e$ by Σ_i . By assumption, Σ_i has measure 1 in G_i^e . Hence, $G_i^e \setminus \Sigma_i$ has measure 0 in G_i^e . Since G_i is open in G , the set $G_i^e \setminus \Sigma_i$ has measure 0 in G^e [FrJ08, Prop. 18.2.4]. It follows that $\bigcup_{i=1}^{\infty} (G_i^e \setminus \Sigma_i)$ has measure 0 in G^e .

If there exists $\sigma \in G^e \setminus \bigcup_{i=1}^{\infty} G_i^e$, then $\langle \sigma \rangle = G$ (otherwise, there exists an i with $\langle \sigma \rangle \leq G_i$, so $\sigma \in G_i^e$, contradicting the assumption on σ). Thus, G is finitely generated, in contrast to the opening statement of the proof. It follows that, $G^e = \bigcup_{i=1}^{\infty} G_i^e$. Hence, $G^e \setminus \bigcup_{i=1}^{\infty} \Sigma_i \subseteq \bigcup_{i=1}^{\infty} (G_i^e \setminus \Sigma_i)$. Therefore, by the preceding paragraph, $G^e \setminus \bigcup_{i=1}^{\infty} \Sigma_i$ has measure 0 in G^e . Consequently, $\bigcup_{i=1}^{\infty} \Sigma_i$ has measure 1 in G^e , so G is almost locally free. \square

Proposition 2.5. *Let K be a Hilbertian field and N a Galois extension of K which is not separably closed. Then $\text{Gal}(N)$ is almost locally free.*

Proof. First we assume that K is countable. Then, so is N . Hence, $\text{rank}(\text{Gal}(N)) \leq \aleph_0$. By Weissauer, each finite proper separable extension of N is Hilbertian [FrJ08, Thm. 13.9.1(b)]. It follows from statement (2) of the introduction that each proper open subgroup of $\text{Gal}(N)$ is almost locally free. Since the absolute Galois group of a Hilbertian field M is not finitely generated (e.g. for each r , the group $(\mathbb{Z}/2\mathbb{Z})^r$ is a quotient of $\text{Gal}(M)$), the group $\text{Gal}(N)$ itself is not finitely generated [FrJ08, Cor. 17.6.3]. Thus, $\text{rank}(\text{Gal}(N)) = \aleph_0$. It follows from Lemma 2.4 that $\text{Gal}(N)$ is almost locally free.

In the general case N has, by Skolem–Löwenheim, a countable elementary subfield M [FrJ08, Prop. 7.4.2]. Let k, l, m be positive integers. By Weissauer, every finite separable proper extension N' of N is Hilbertian. Hence, for every irreducible separable polynomial $p \in N[X]$ with $2 \leq \deg(p) \leq k$, for each extension N' of N generated by a root of p , for every irreducible polynomial $f \in N'[T, X]$ separable in X of degree $\leq l$, and for every $g \in N'[T]$ with $g \neq 0$ and $\deg(g) \leq m$, there exists $a \in N'$ such that $f(a, X)$ is irreducible in $N'[X]$ and $g(a) \neq 0$. The latter statement is an elementary statement on N , that is, it is equivalent to a first order sentence in the language of rings with parameters in N . Since M is an elementary subfield of N , the same statement holds over M . Thus, every finite separable proper extension of M is Hilbertian. Applying the arguments of the preceding paragraph to M rather than N , we conclude that $\text{Gal}(M)$ is almost locally free.

Finally we observe that N/M is a regular extension, because M is an elementary subfield of N [FrJ08, Example 7.3.3]. Hence, $\text{res} : \text{Gal}(N) \rightarrow \text{Gal}(M)$ is an epimorphism. It follows from Example 2.2 that $\text{Gal}(N)$ is locally free. \square

We prove the analog of Proposition 2.5 for free profinite groups.

Proposition 2.6. *Let F be a free profinite group of rank ≥ 2 . Then every nontrivial closed normal subgroup N of F is almost locally free.*

Proof. If N is open in F , then so is every open subgroup N' of N . By [FrJ08, Prop. 17.6.2], N' is free of rank ≥ 2 . Hence, by Example 2.1, N' is almost locally free. Thus, we may assume that $(F : N) = \infty$.

If $2 \leq \text{rank}(F) < \aleph_0$, then by [Jar06, Prop. 1.3], every proper open subgroup N' of N is free of infinite rank. Again, by Example 2.1, N' is almost locally free. Hence, by Lemma 2.4, N is locally free.

If $\text{rank}(F) \geq \aleph_0$, we use that F is projective [FrJ08, Cor. 24.4.5] and a result of Lubotzky–v.d. Dries [FrJ08, Cor. 23.1.2] to find a PAC field K such that $F \cong \text{Gal}(K)$. By [FrJ08, Lemma 25.1.1], F is ω -free. Hence, by Roquette, K is Hilbertian [FrJ08, Cor. 27.3.3]. It follows from Proposition 2.5 that N is almost locally free. \square

Problem 2.7. Give an example for an almost ω -free profinite group that is not almost locally free.

References

- [FrJ08] M.D. Fried, M. Jarden, *Field Arithmetic*, third edition, *Ergeb. Math. Grenzgeb.* (3), vol. 11, Springer, Heidelberg, 2008, revised by Moshe Jarden.
- [HaL82] D. Haran, A. Lubotzky, Embedding covers and the theory of Frobenius fields, *Israel J. Math.* 41 (1982) 181–202.
- [Hrb94] D. Harbater, Abhyankar’s conjecture on Galois groups over curves, *Invent. Math.* 117 (1994) 1–25.
- [HrS11] D. Harbater, K. Stevenson, Embedding problems and open subgroups, *Proc. Amer. Math. Soc.* 139 (2011) 3335–3349.
- [Iwa53] K. Iwasawa, On solvable extensions of algebraic number fields, *Ann. of Math.* 58 (1953) 548–572.
- [Jar74] M. Jarden, Algebraic extensions of finite corank of Hilbertian fields, *Israel J. Math.* 18 (1974) 279–307.
- [Jar06] M. Jarden, A Karrass–Solitar theorem for profinite groups, *J. Group Theory* 9 (2006) 139–146.
- [Kuy68] W. Kuyk, Generic approach to the Galois embedding and extension problem, *J. Algebra* 9 (1968) 393–407.
- [Lub93] A. Lubotzky, Random elements of a free profinite group generate a free subgroup, *Illinois J. Math.* 37 (1993) 78–84.